Homeland Security

Information Analysis Infrastructure Protection

Protected Critical Infrastructure Information Program

Fact Sheet

The Protected Critical Infrastructure Information (PCII) Program, established pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), creates a new framework which enables members of the private sector to, for the first time, voluntarily submit confidential information regarding the nation's critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure.

The PCII Program seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism.

To implement and manage the program, DHS has created the PCII Program Office within the Information Analysis and Infrastructure Protection (IAIP) Directorate. The PCII Program Office will receive critical infrastructure information and evaluate it to determine whether it qualifies for protection under the CII Act.

Why was the program created?

An essential element of ensuring homeland security is the protection of the nation's critical infrastructures by federal, state, local, and private sector efforts. These infrastructures are the systems, assets, and industries upon which our national security, economy, and public health depends. It is estimated that over 85% of the critical infrastructure is owned and operated by the private sector. Recognizing that the private sector may be reluctant to share information with the Federal Government if it could be publicly disclosed, Congress passed the CII Act in 2002 with its provisions for protection from public disclosure.

Why should private industry voluntarily submit this information?

The security and protection of the Nation's critical infrastructure are of paramount importance, not only to the federal, state and local governments, but also to private utilities, businesses, and industries. There are several benefits for private sector participants in the PCII program:

- Proprietary, confidential, or sensitive infrastructure information can now be shared with governmental entities who share the private sector's commitment to a more secure homeland.

- Information sharing will result in better identification of risks and vulnerabilities, which will help industry partner with others in protecting their assets.
- By voluntarily submitting CII to the Federal Government, industry is helping to safeguard and prevent disruption to the American economy and way of life.
- Private industry is demonstrating good corporate citizenship that may save lives and protect communities.

How will protected critical infrastructure information be used?

PCII may be used for many purposes, focusing primarily on analyzing and securing critical infrastructure and protected systems, risk and vulnerabilities assessments, and assisting with recovery as appropriate. The IAIP Directorate plays a critical role in securing the homeland by identifying and assessing threats and mapping those threats against vulnerabilities such as critical infrastructure.

What information do submitters provide to the PCII Program Office?

Submissions must include the following:

- ✓ An Express Statement requesting CII Act protection
- ✓ A Certification Statement
- ✓ An affirmation of the understanding of the submitter that any false representations on submissions may constitute a violation of 18. U.S.C 1001 and be punishable by fine and imprisonment

Information on the wording of the Express Statement and guidelines for the Certification Statement are available on the PCII Program web site at www.DHS.gov.

What is the process for determining if CII will be designated as protected?

Once the package is received from submitters, PCII Program Office staff will determine if the package contains an Express Statement requesting the protection of the CII Act. If it does not include the Express Statement, it is returned to the sender.

If the package contains the Express Statement, PCII Program Office staff will determine if the submittal meets the requirements for protection in the CII Act and regulations, 6 CFR Part 29. The PCII Program Office will notify the submitter upon receipt and once a validation determination has been made.

If the information is determined not to qualify for PCII protection, the Program Office will contact the submitter and ask for additional justification. During the entire process of determining whether the information qualifies for protection under the CII Act, the submitted information will be presumed to be, and will be treated as, PCII.

For additional information on the PCII Program and how to submit CII to the Office, visit the web site at www.DHS.gov

For additional information on the PCII Program and how to submit CII to the Office, visit the web site at: www.DHS.gov